



Банк России

ОБЗОР ОСНОВНЫХ ТИПОВ
КОМПЬЮТЕРНЫХ АТАК
В ФИНАНСОВОЙ СФЕРЕ
В 2025 ГОДУ

ОГЛАВЛЕНИЕ

1. Источники данных.....	2
2. Аналитика ландшафта киберугроз	4
2.1. Кого и чем атаковали чаще всего.....	4
2.2. Векторы атак.....	5
2.3. Типовая схема компьютерного инцидента.....	11
3. Киберучения	17
4. Тенденции 2026 года	18

Обзор подготовлен Департаментом информационной безопасности.
При использовании материалов выпуска ссылка на Банк России обязательна.

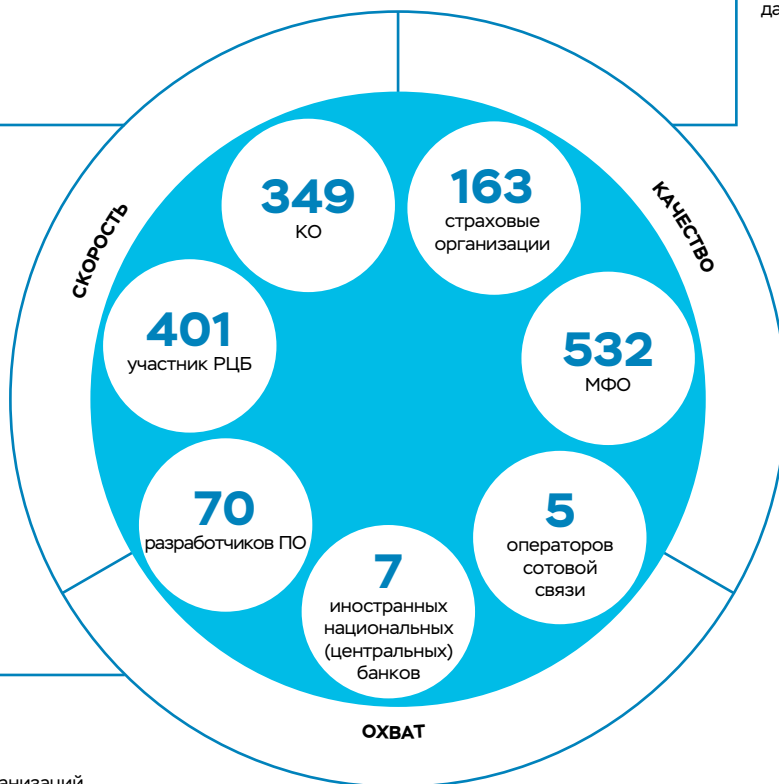
107016, Москва, ул. Неглинная, 12, к. В
Официальный сайт Банка России: www.cbr.ru

© Центральный банк Российской Федерации, 2026

1. ИСТОЧНИКИ ДАННЫХ

Не более 1 часа* занимает реагирование ФинЦЕРТ на ИБ-инцидент на финансовом рынке

8,4 из 10** – такую оценку поставили участники информационного обмена качеству предоставляемых данных ФинЦЕРТ



Участвовало:

- Более 1 700 организаций

Выявлено:

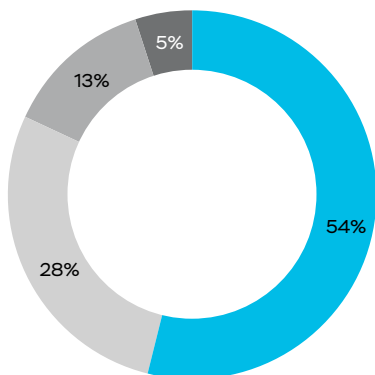
- 38 418 фишинговых сайтов (направлено на блокировку)
- 761 инцидент операционной надежности (ОН)
- 14 инцидентов у подрядных организаций с последующими атаками на финансовый рынок

* Скорость первичной обработки дежурным ФинЦЕРТ входящего запроса.

** По данным проведенного опроса участников финансового рынка в 2025 году.

Распределение по типам компьютерных атак¹ и инцидентов², направленных на финансовые организации в 2025 году (по данным ФинЦЕРТ)

Распределение по типам компьютерных атак

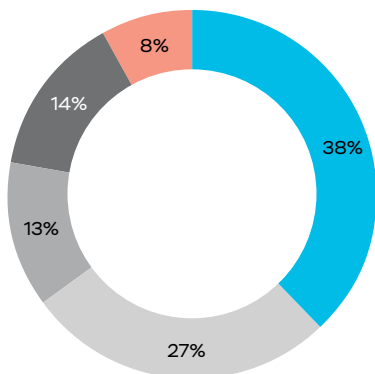


- Иные атаки (компрометация аутентификационных или учетных данных, изменение маршрутно-адресной информации, эксплуатация уязвимостей, сканирование портов и другие)
- Атаки типа «отказ в обслуживании»
- Использование вредоносного ПО
- Фишинговая рассылка

296

DDoS-атак зафиксировано ФинЦЕРТ

Распределение по типам компьютерных инцидентов



- Заражение вредоносным ПО
- Шифрование инфраструктуры
- Утечка данных
- Несанкционированный доступ к ресурсу
- Компрометация учетной записи

В 10 ФИНАНСОВЫХ ОРГАНИЗАЦИЯХ

произошли инциденты, связанные с вирусом-шифровальщиком³

¹ Компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

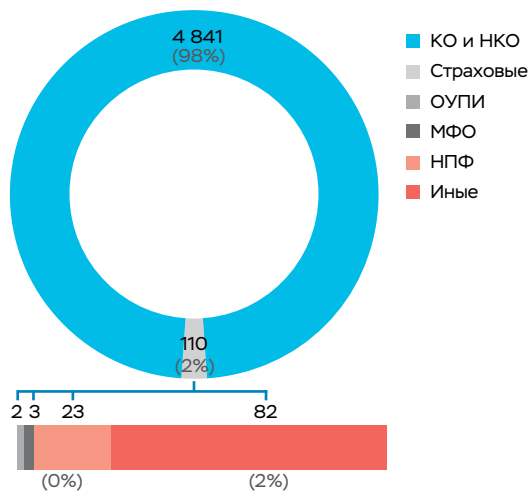
² Компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, произошедший в том числе в результате компьютерной атаки.

³ Вирус-шифровальщик (Ransomware) – вредоносное ПО, блокирующее пользователю доступ к файлам путем их шифрования.

2. АНАЛИТИКА ЛАНДШАФТА КИБЕРУГРОЗ

2.1. Кого и чем атаковали чаще всего

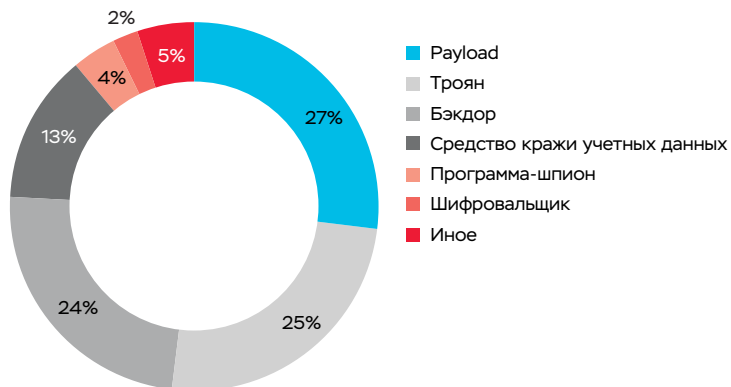
Количество атак по типам организаций



ФОКУС НА ПРЕДСТАВИТЕЛЯХ МАЛЫХ И СРЕДНИХ ОРГАНИЗАЦИЙ – ПОСТАВЩИКОВ ИТ-УСЛУГ

За счет атак на менее крупные организации атакующие экономят время и ресурсы, рассчитывая в дальнейшем получить доступ к инфраструктуре крупной организации, если она взаимодействовала со скомпрометированным подрядчиком.

Распределение типов ВПО в 2025 году



УВЕЛИЧЕНИЕ КОЛИЧЕСТВА АТАК С ИСПОЛЬЗОВАНИЕМ МОДЕЛИ RaaS (RANSOMWARE AS A SERVICE)

Злоумышленники могут модифицировать существующие инструменты под новые задачи или взять их в пользование (аренду).

2.2. Векторы атак⁴

2.2.1. Третья сторона – поставщики (провайдеры) ИТ-услуг / ИБ-услуг, провайдеры связи, ЦОД

В 2025 году количество целевых атак на участников финансовой сферы осталось на стабильно высоком уровне. При этом увеличилось и количество атак на менее защищенную ИТ-инфраструктуру поставщиков и сервисных компаний (сервис-провайдеров), предлагающих широкий спектр услуг по оптимизации технологической и операционной деятельности финансовых организаций либо выполняющих сервисное обслуживание с возможностью удаленного подключения. В подобных условиях кредитные организации принимают на себя риск возможной компьютерной атаки на свою инфраструктуру через привлеченную внешнюю компанию. Поэтому организации финансовой сферы должны проводить тщательный анализ модели угроз такого взаимодействия, корректировать параметры риск-ориентированного управления им, а также реализовывать соответствующие организационные и технические мероприятия противодействия таким угрозам.

Соблюдение рекомендаций при организации рабочих взаимоотношений с поставщиками услуг значительно снижает риски проведения атак через третьи стороны



⁴ Вектор атаки – путь, используемый злоумышленником для проникновения в информационную инфраструктуру жертвы, обхода защиты и несанкционированного доступа.

2.2.2. Аналитика уязвимостей в программных продуктах на основе международных данных

В 2025 году использование уязвимостей ПО являлось одним из первоначальных векторов атак на организации финансовой сферы, а также других сфер экономики.

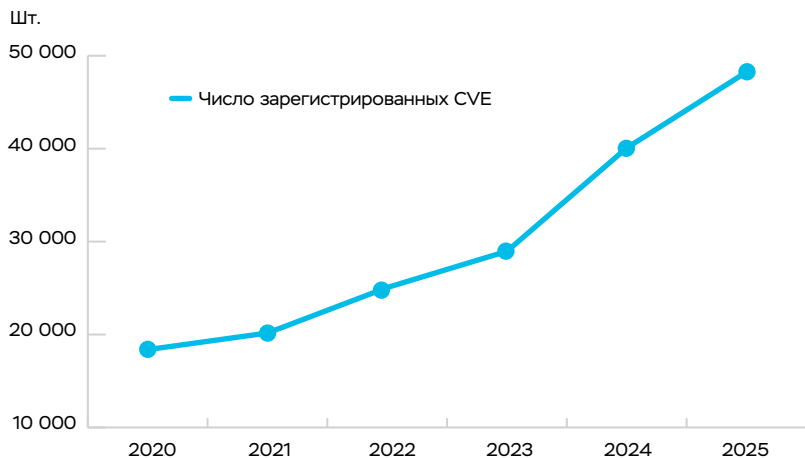
По данным, имеющимся в распоряжении ФинЦЕРТ, в большинстве компьютерных инцидентов в качестве точки входа в инфраструктуру организации использовались уязвимости программного продукта Bitrix, обнаруженные еще в 2023 году.

Тенденция и попытки атак с использованием уязвимостей в программном продукте семейства 1С-Bitrix сохраняются. Проводимая ФинЦЕРТ активная работа по информированию участников финансового рынка об уязвимостях в данном ПО способствовала значительному снижению количества связанных с ним инцидентов. Тем не менее в 2025 году зафиксированы случаи эксплуатации уязвимостей в 1С-Bitrix в организациях кредитно-финансовой сферы.

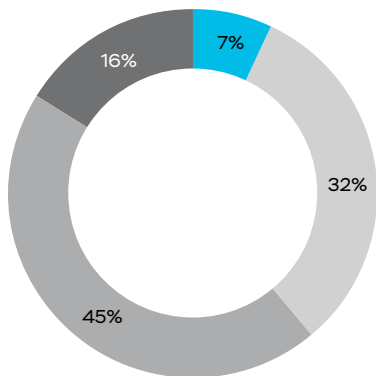
ФинЦЕРТ на постоянной основе публикует информацию об актуальных и эксплуатируемых уязвимостях ПО в кредитно-финансовой сфере и оповещает участников в своих еженедельных дайджестах, информационных и оперативных бюллетенях об их возможном использовании злоумышленниками, дает рекомендации по мерам противодействия.

Своевременная обработка поступающих от ФинЦЕРТ сведений и реагирование на них позволяют организациям – участникам информационного обмена оперативно отвечать на угрозы кибербезопасности, а также предотвращать возможные компьютерные инциденты.

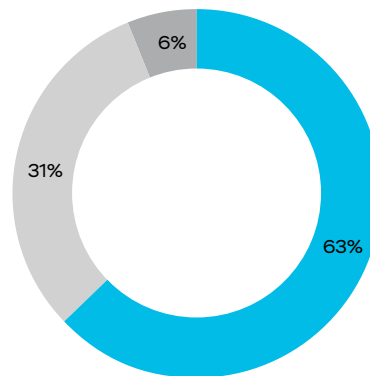
Глобальный рост числа CVE 2025

**+20%**к числу уязвимостей
по сравнению с 2024 годом**БОЛЕЕ
48 000**

уязвимостей в 2025 году

Степень критичности уязвимостей
по CVSS 2025

- Критическая (9-10)
- Высокая (7,0-8,9)
- Средняя (4,0-6,9)
- Низкая / без оценки (< 4,0)

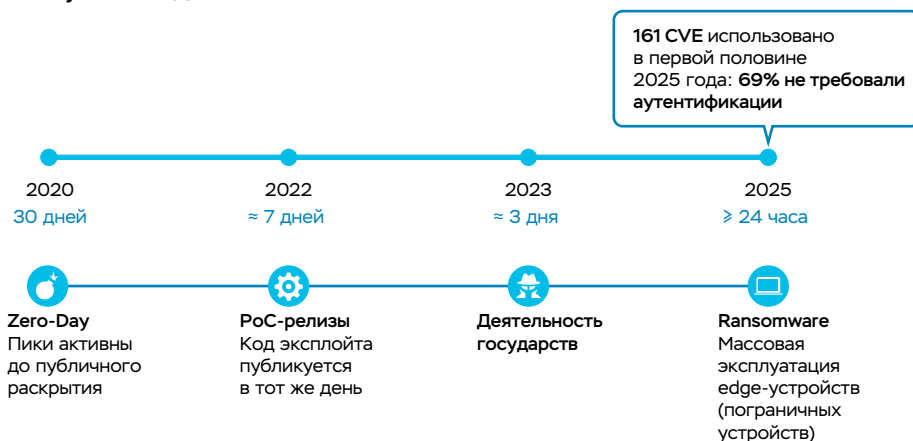
Распределение уязвимостей
по вендорам в 2025 году

- ОС и ПО семейства Microsoft
- Архиваторы 7-Zip и WinRAR
- ПО 1С-Bitrix

В 2025 году наибольшее число атак на организации финансовой сферы с использованием уязвимостей ПО пришлось на следующие группы производителей ПО:

1. **CVE-2025-24071** – эксплуатация уязвимости позволяет неавторизованному злоумышленнику перехватывать NTLM-хеш-суммы.
2. **CVE-2025-49704, CVE-2025-49706, CVE-2025-53770, CVE-2025-53771** – уязвимости в Microsoft SharePoint, связанные с десериализацией недоверенных данных.
3. **CVE-2024-35250** – уязвимость связана с разыменованием недоверенного указателя и позволяет выполнять произвольный код.
4. **CVE-2020-1472 (Zerologon)** – позволяет атакующему скомпрометировать учетную запись машинного аккаунта контроллера домена и получить доступ к содержимому всей базы Active Directory.
5. **CVE-2017-11882, CVE-2018-0802** – уязвимости в редакторе уравнений из пакета Microsoft Office.
6. **CVE-2017-0199** – уязвимость в Microsoft Office и WordPad.
7. **CVE-2023-38831, CVE-2025-6218, CVE-2025-8088** – уязвимости, связанные с выходом за пределы назначенного каталога в WinRAR.
8. **CVE-2025-11001, CVE-2025-11002** – уязвимости файлового архиватора 7-Zip связаны с неверным определением символических ссылок перед доступом к файлу.
9. **CVE-2022-27228** – критическая уязвимость CMS 1C-Bitrix.

Сокращение сроков выявления и эксплуатации злоумышленниками уязвимостей «нулевого дня»



Коллапс скорости эксплуатации – атакующие теперь превращают новые уязвимости в средство атаки в течение нескольких часов после публичного раскрытия.

24 ЧАСА

В начале 2025 года примерно 28% зафиксированных случаев эксплуатации уязвимостей были совершены в течение суток после их обнаружения. Это означает, что к моменту публикации исправления уязвимости или иного уведомления злоумышленники уже начинают сканирование и компрометацию незащищенных систем.

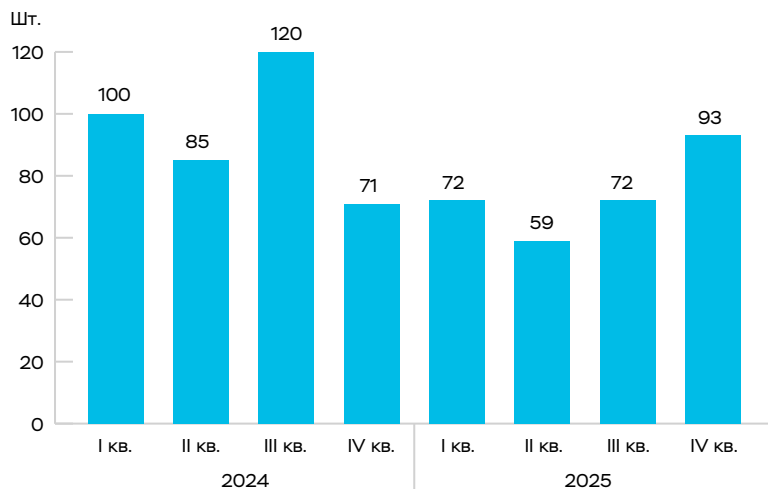
БОЛЕЕ 160 УЯЗВИМОСТЕЙ ИСПОЛЬЗОВАЛИ ЗЛОУМЫШЛЕННИКИ В ПЕРВОМ ПОЛУГОДИИ 2025 ГОДА

Среди них были как новые уязвимости «нулевого дня», так и старые ошибки, которые организации не исправляли. Примерно для 42% эксплуатируемых CVE существовали общедоступные эксплойты либо тестовые образцы (PoC), что значительно снижало время, необходимое для проведения масштабных атак.

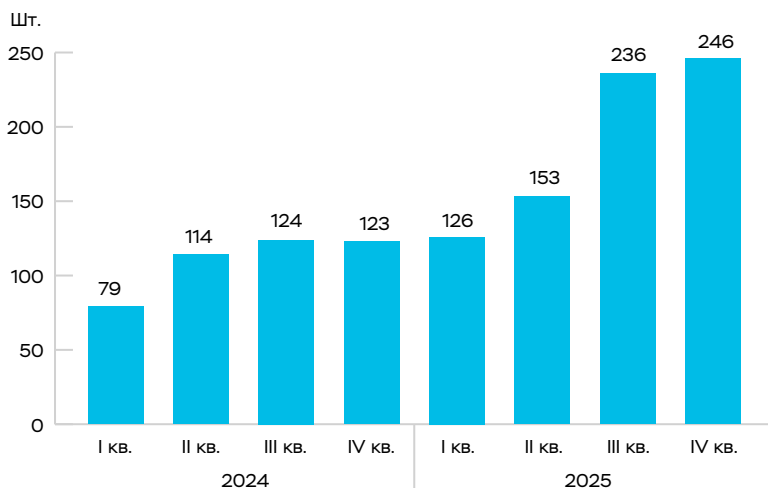
69% эксплуатируемых уязвимостей не требовали аутентификации (например, могли быть удаленно использованы любым пользователем сети Интернет), а около 30% позволяли удаленно выполнять код (RCE).

2.2.3. DDoS-атаки

Динамика DDoS-атак



Динамика инцидентов операционной надежности



296 DDoS-АТАК

совершено в 2025 году,
что на 21% меньше
показателя 2024 года

КАЖДАЯ 9-Я DDoS-АТАКА

привела к инциденту ОН
(36 инцидентов ОН стали
последствием DDoS-атак)

4 ДНЯ отсутствовал доступ
к сервисам финансовой
организации в результате
DDoS-атаки

НАРУШЕНИЕ ДОСТУПНОСТИ УСЛУГ И СЕРВИСОВ, В ТОМ ЧИСЛЕ DDoS

1 717

выявленных событий,
предположительно, связанных
со сбоями

963

подтвержденных сбоя

761

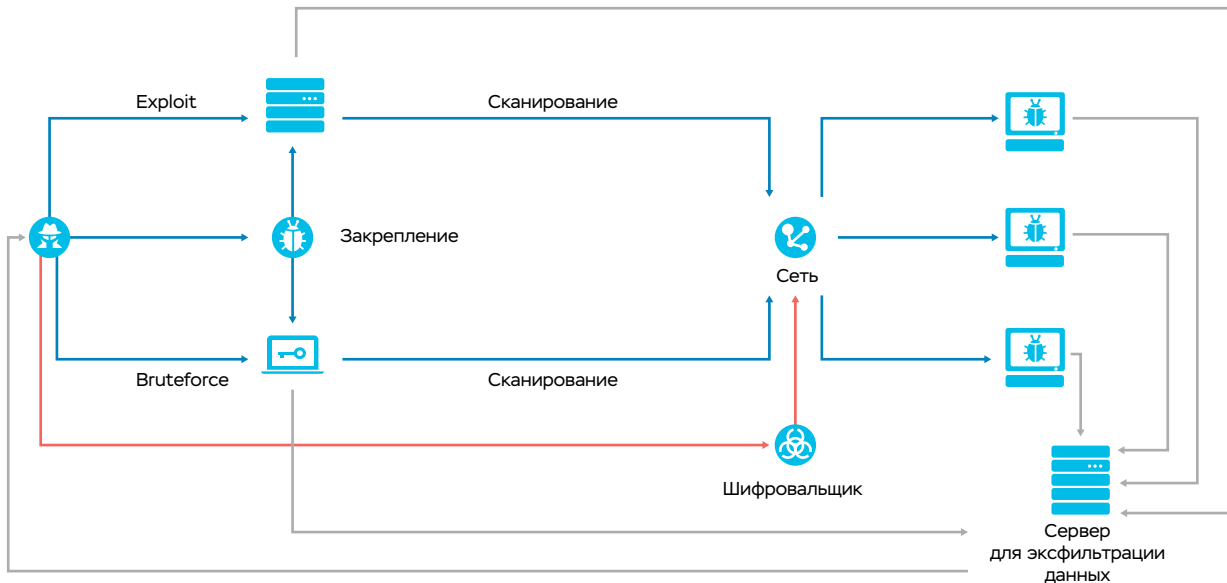
инцидент ОН

166

дней – общая продолжительность
инцидентов ОН, выявленных
в 2025 году

2.3. Типовая схема компьютерного инцидента

В 2024 году наблюдались многовекторные и сложные атаки. В 2025 году типовая атака на организацию выглядела следующим образом:



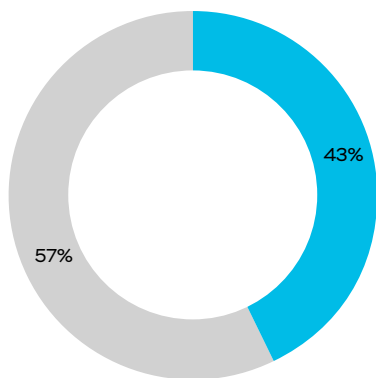
1. Получение первоначального доступа за счет эксплуатации уязвимости / перебор связки «логин-пароль».
2. Закрепление в инфраструктуре за счет добавления процесса в автозапуск / установка средства туннелирования.
3. Сбор информации об инфраструктуре доступных данных.
4. Горизонтальное перемещение (там, где возможно).
5. Эксfiltrация данных.
6. Шифрование инфраструктуры.

В рамках проведения компьютерных атак злоумышленники стали чаще эксплуатировать ПО, используемое командами Red Team⁵, а также доступное ПО для выявления уязвимостей и общесистемные утилиты операционных систем, все меньше прибегая к самостоятельной разработке вредоносного ПО.

Кроме того, за 2025 год не было выявлено новых типов семейств шифровальщиков, задействованных в атаках на финансовый сектор. Зафиксировано значительное число атак с использованием шифровальщиков, исходный код которых находится в открытом доступе.

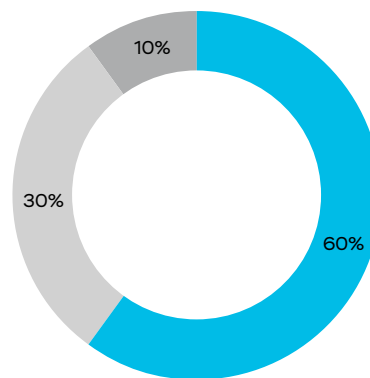
2.3.1. Шифровальщики

Инциденты за 2025 год



■ Шифровальщики
■ Остальное

Вирусы-шифровальщики, зафиксированные в рамках реагирования на инциденты в 2025 году



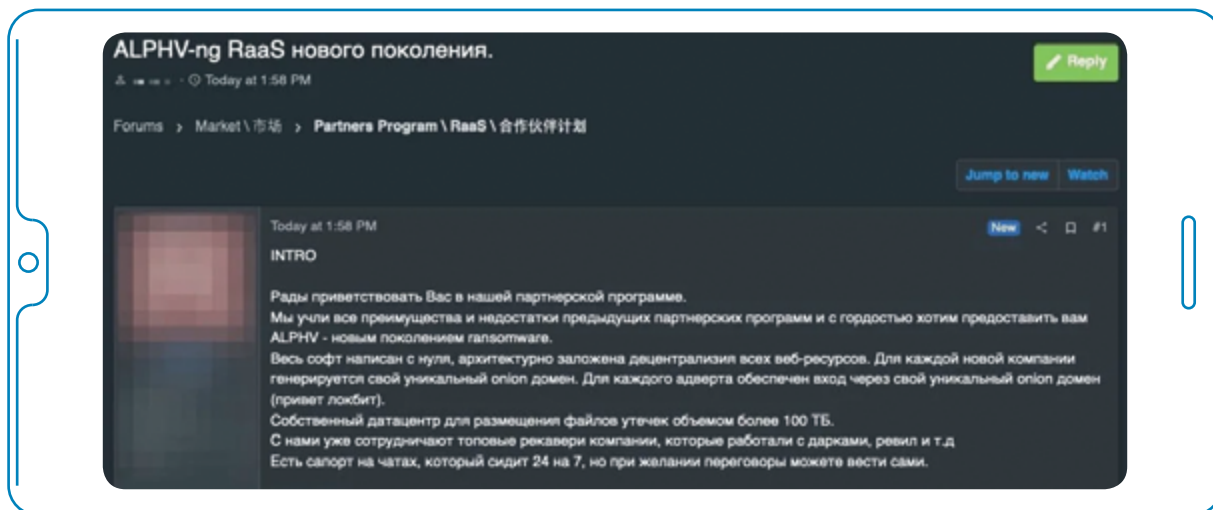
■ Babuk
■ Lockbit
■ Иное

⁵ Red Team – группа экспертов по кибербезопасности, имитирующих реальные, скрытые и многоступенчатые атаки на инфраструктуру компании для проверки эффективности ее защиты.

На основе имеющейся в ФинЦЕРТ информации в 2025 году Банк России фиксирует увеличение количества инцидентов в организациях финансового сектора, результатом которых являлось шифрование их инфраструктуры.

Если раньше такие атаки осуществлялись, чтобы получить выкуп, то ближе к концу 2025 года их целью стало нанесение максимального урона инфраструктуре организации.

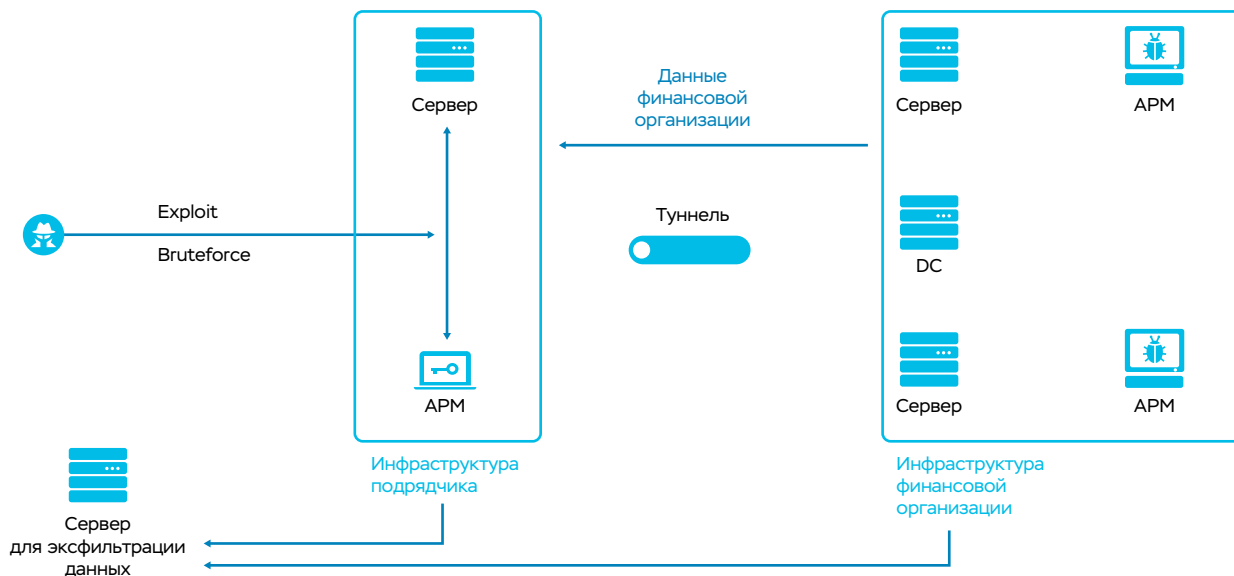
Рост количества инцидентов можно связать с набирающей в теневом сегменте сети Интернет моделью продажи услуг RaaS, а также, как отмечалось в годовом отчете ФинЦЕРТ о компьютерных атаках на финансовый сектор за 2024 год, с выложенным исходным кодом шифровальщиков семейств Babuk⁶ и LockBit⁷. Пример объявления с одного из теневых ресурсов:



⁶ Babuk – семейство программ-вымогателей, использующее тактику двойного вымогательства. Впервые обнаружено в 2021 году.

⁷ LockBit – одно из наиболее активных семейств ВПО класса RaaS (шифровальщик как услуга). Впервые обнаружено в 2019 году.

Обобщенная схема типовой атаки с использованием вируса-шифровальщика



1. Атакующий изучает инфраструктуру подрядной организации, определяя уязвимые места. В основном точкой входа является эксплуатация уязвимости ПО либо использование словарного пароля к учетной записи.
2. Атакующий закрепляется в инфраструктуре подрядной организации, проводит горизонтальное перемещение, чтобы захватить как можно больше серверов и APM.
3. После закрепления в инфраструктуре атакующий проводит исследование доступных информационных ресурсов с целью выявления среди них тех, которые позволяют организовать распространение в инфраструктуру другой организации (целевая организация – основная цель атаки), с которой осуществляется взаимодействие. Это могут быть как связки «логин-пароль», так и технические данные, например ключи ssh⁸.
4. В случае обнаружения такой информации атакующий использует полученную информацию для проникновения в инфраструктуру целевой организации, закрепляясь в ней.
5. В качестве резервного канала обмена данными устанавливается средство туннелирования между инфраструктурами двух организаций, реже – между управляющим сервером (CnC) атакующего и скомпрометированной инфраструктурой через подрядчика организации.

⁸ Ключи ssh – пара криптографических файлов (открытый и закрытый), используемых для безопасной аутентификации на удаленном сервере без пароля.

6. Проводится исследование сетевых и информационных ресурсов целевой организации, определение мест хранения и обработки данных, параметров учетных записей, используемого ПО, а также используемых средств ИБ. На данном этапе атакующий старается получить доступ к серверам, критичным для функционирования целевой организации, мест размещения информационных данных. В основном это контроллеры домена, сервера СУБД, инфраструктура резервного копирования информационных данных и средств учета и конфигурирования ПО ИТ-инфраструктуры.
7. После того как атакующий закончил сбор данных со всех устройств, до которых удалось добраться, либо атакующий понял, что его активность была обнаружена, запускается процесс шифрования данных.

В ходе эксфильтрации данных атакующий может начать выгружать данные как на свой сервер, так и на сервер организации, через которую осуществлялась атака.

Несмотря на деструктивность воздействия подобных атак, во всех случаях финансовые организации смогли восстановить свою инфраструктуру и клиентские сервисы в максимально короткие сроки. В исключительных случаях атакующим удавалось добраться до резервных копий систем, тогда срок восстановления работоспособности инфраструктуры увеличивался.

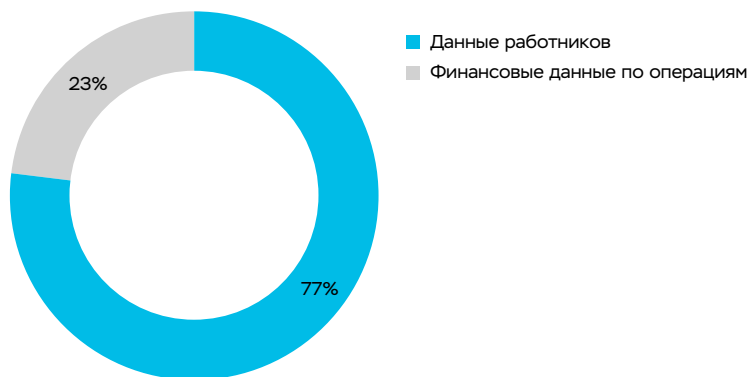
В качестве мер по защите от подобных атак рекомендуется:

- использовать обновляемое ПО, в котором закрываются обнаруженные уязвимости;
- внедрять в инфраструктуру современные СЗИ;
- организовать резервное копирование таким образом, чтобы в случае атаки до резервных копий нельзя было добраться из локальной сети;
- внедрять концепцию нулевого доверия для «внешних» учетных записей, а также ограничения работы служб RDP⁹;
- использовать многофакторную аутентификацию для доступа в инфраструктуру;
- внедрять строгую парольную политику в отношении как технических учетных записей, так и учетных записей пользователей;
- проводить обучение сотрудников основам ИБ.

⁹ Служба RDP – сетевой протокол для организации удаленной работы пользователя с сервером.

2.3.2. Утечки данных

Утечки конфиденциальной информации в 2025 году



В 2025 году, по данным ФинЦЕРТ, количество крупных утечек конфиденциальной информации в компаниях кредитно-финансовой отрасли снизилось. Тем не менее в результате атак с использованием вредоносного ПО на подрядные организации были зафиксированы случаи появления в свободном доступе информации, имеющей отношение к деятельности финансовых организаций. Данный факт подтверждает смещение вектора от проведения злоумышленниками прямых целевых атак на финансовые организации к атакам на менее защищенные инфраструктуры поставщиков услуг и сервисных компаний.

3. КИБЕРУЧЕНИЯ

Киберучения

За последние 3 года

987

организаций
участвовали
в киберучениях

> 30 000

фишинговых
писем направлено

> 30

сценариев
отработано

Цели киберучений

- Повышение качества реагирования на целевые компьютерные атаки
- Повышение скорости взаимодействия с ФинЦЕРТ
- Отработка действий по обеспечению безопасности информационной инфраструктуры финансовыми организациями

Рассматриваемые сценарии

Выводы

- Каждая организация, участвуя в киберучениях Банка России, выявляет недостатки во внутренних бизнес-процессах и вносит изменения в том числе в сценарии киберучений

Рекомендации

- Банк России ориентирует финансовые организации на улучшение конкретных показателей реагирования на выявляемые угрозы



Эксплуатация уязвимостей

Проверка скорости исправления выявленных уязвимостей и внешнего взаимодействия



Фишинговые рассылки

Проверка знаний ИБ работников организаций. Корректность реагирования на внешнюю угрозу



Хищение денежных средств

Проверка готовности организаций к оперативному взаимодействию с ФинЦЕРТ. Наличие конкретных процедур

В 2025 ГОДУ В УЧЕНИЯХ ПРИНЯЛИ УЧАСТИЕ БОЛЕЕ 320 ОРГАНИЗАЦИЙ, ЧТО НА 10% БОЛЬШЕ, ЧЕМ ГОДОМ РАНЕЕ. В 6,5% ФИНАНСОВЫХ ОРГАНИЗАЦИЙ РАБОТНИКИ БЫЛИ УСЛОВНО СКОМПРОМЕТИРОВАНЫ, ЧТО ГОВОРИТ ОБ ОТНОСИТЕЛЬНО ВЫСОКОМ УРОВНЕ ПОДГОТОВКИ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ К ПРОТИВОДЕЙСТВИЮ ТАКОГО ВЕКТОРА АТАКИ.

ВСЕГО ЗА ВРЕМЯ ПРОВЕДЕНИЯ КИБЕРУЧЕНИЙ БЫЛИ УСЛОВНО СКОМПРОМЕТИРОВАНЫ 25 РАБОТНИКОВ В 21 ФИНАНСОВОЙ ОРГАНИЗАЦИИ.

4. ТЕНДЕНЦИИ 2026 ГОДА

На основе анализа компьютерных инцидентов на инфраструктуре участников финансовой сферы, а также по результатам проведенного анализа компьютерных атак наиболее актуальными в 2026 году могут стать следующие угрозы:

- **Активность шифровальщиков.** Количество атак с использованием шифровальщиков будет только расти. Однако стоит отметить тенденцию изменения целей таких атак: если раньше атаки были связаны с вымогательством финансовых средств, то сейчас они начинают носить деструктивный характер. Это значит, что получение выкупа больше не является целью атакующих. Сейчас они стараются нанести максимальный вред организации за счет остановки рабочих процессов, а также максимального освещения инцидента в сети Интернет.
- **Использование искусственного интеллекта.** В связи с тем что атаки при помощи ИИ имеют высокий уровень автоматизации и невысокий входной порог уровня технической подготовки, их количество может увеличиваться. Атаки с использованием ИИ позволяют как проводить массовые рассылки фишинговых ссылок и ВПО, так и внедряться в инфраструктуру.
- **Смещение вектора атаки в сторону кражи данных.** Кража данных пользователей – распространенная цель атаки. Однако если раньше украденные данные использовались с целью вымогательства и нанесения репутационного ущерба, то сейчас, если среди украденных данных есть, например, корпоративные данные, атакующие могут использовать их для дальнейшего развития атаки на организацию.
- **Атаки на средние и малые организации.** Подобные атаки встречались в 2025 году очень часто. В результате компрометации менее крупных компаний, имеющих удаленный доступ к инфраструктуре других организаций в рамках оказания услуг, атакующие получали доступ в инфраструктуру более крупных компаний. Таким образом, тенденция атак на малый и средний бизнес сохранится.

- **Развитие банковских троянов и ВПО для мобильных устройств.** ПО для скрытого управления мобильным устройством постоянно модифицируются, что усложняет процесс их обнаружения. Операционные системы мобильных устройств обеспечивают доступ к каналу СМС / пуш-уведомлений (подтверждений), что облегчает скрытый перехват и модификацию сообщений при работе с ДБО. Методы кражи с помощью мобильных устройств постоянно развиваются, что требует повышенного внимания к обеспечению безопасности взаимодействия клиента с ДБО через мобильное устройство.

Киберучения с финансовыми организациями

Расширение географии киберучений, а также ввод дополнительных сценариев

Анализ угроз подрядчиков по категориям

Участие поставщиков ИТ-решений в информационном обмене с АСОИ ФинЦЕРТ

База ИОС с постоянным доступом

Планируется автоматизация получения ИОС участниками АСОИ ФинЦЕРТ



**2026
ГОД**